Livre blanc • Octobre 2017

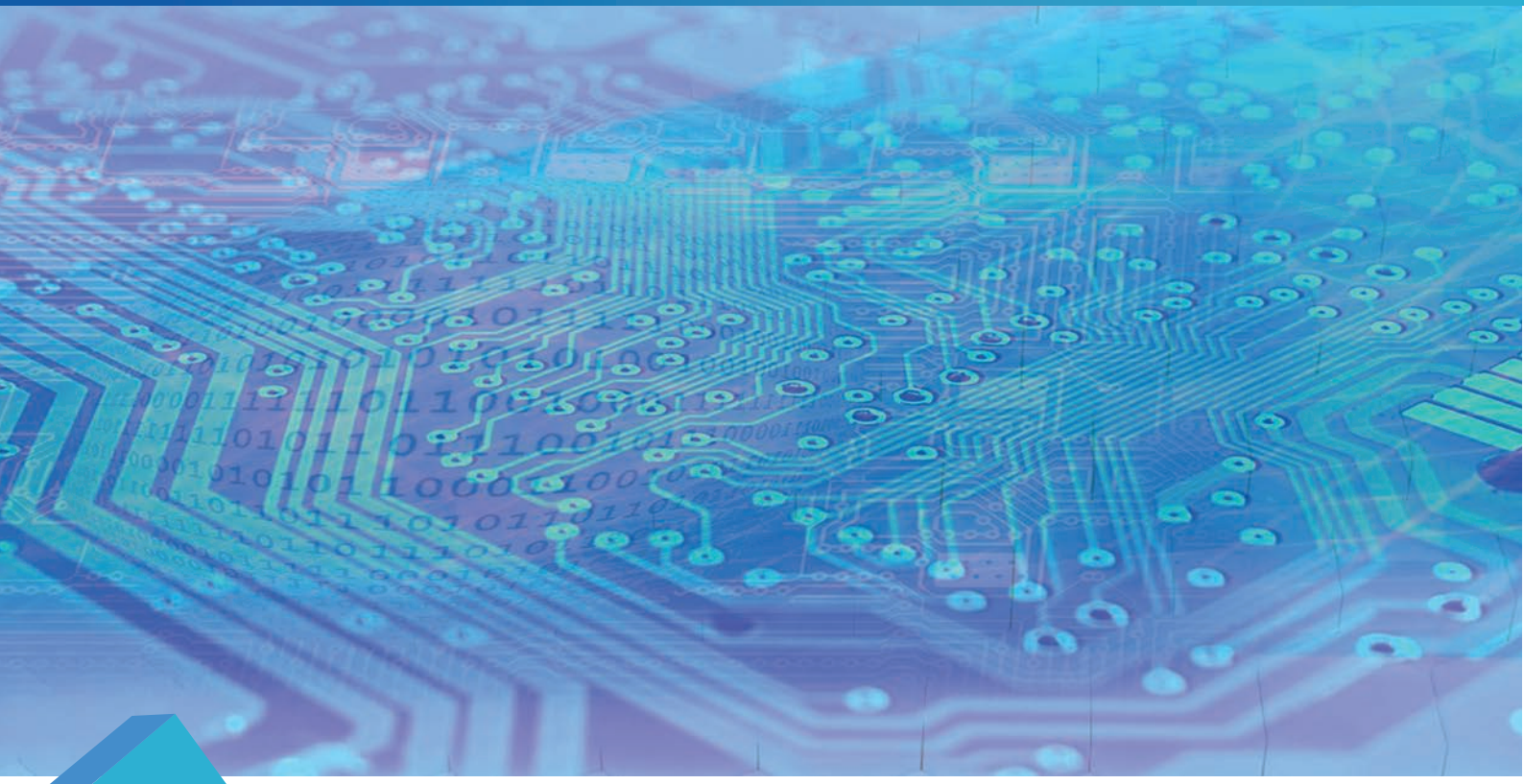
La cybersécurité : des réponses adaptées

LEMONDE INFORMATIQUE

DCI Because we know it

cisco Premier Partner

1. Les nouveaux usages : cibles privilégiées des cybercriminels



Les Clouds, la mobilité, les Big Data, les objets connectés, les expériences utilisateurs et même les intelligences artificielles à venir, toutes ces technologies numériques qualifiées de nouveaux usages - encore plus ou moins adoptées pour certaines - transforment et vont transformer considérablement les entreprises dans leur organisation et dans leur fonctionnement. A ce titre, il existe déjà une vraie prise de conscience des usages du numérique de la part des entreprises pour changer l'environnement de travail des utilisateurs. Selon l'étude intitulée Digital Workplace in Europe et réalisée par le cabinet Pierre Audoin Consultants (PAC), 42 % des responsables IT et RH (ressources humaines) placent la transformation numérique de l'environnement de travail comme une priorité de leurs prochains investissements et 63 % des entreprises sondées prévoient même d'investir dans les technologies citées précedemment dans les deux ans. Mais l'adoption du numérique dans l'entreprise engendre aussi une architecture IT, certes plus flexible, mais aussi plus ouverte et donc plus vulnérable aux cybercriminels. L'enjeu de la cybersécurité est donc une priorité. Depuis quelques années, les attaques de grande ampleur se sont d'ailleurs multipliées faisant souvent la une des journaux notamment celle de TV5 Monde le 8 avril 2015 dont les équipes ont perdu le contrôle des 12 chaînes du groupe pendant plusieurs mois. Résultat : un coût estimé à près de 5 millions d'euros. Dans le monde, le coût des cyberattaques avoisine même les 380 milliards d'euros selon le cabinet PwC.

27 %

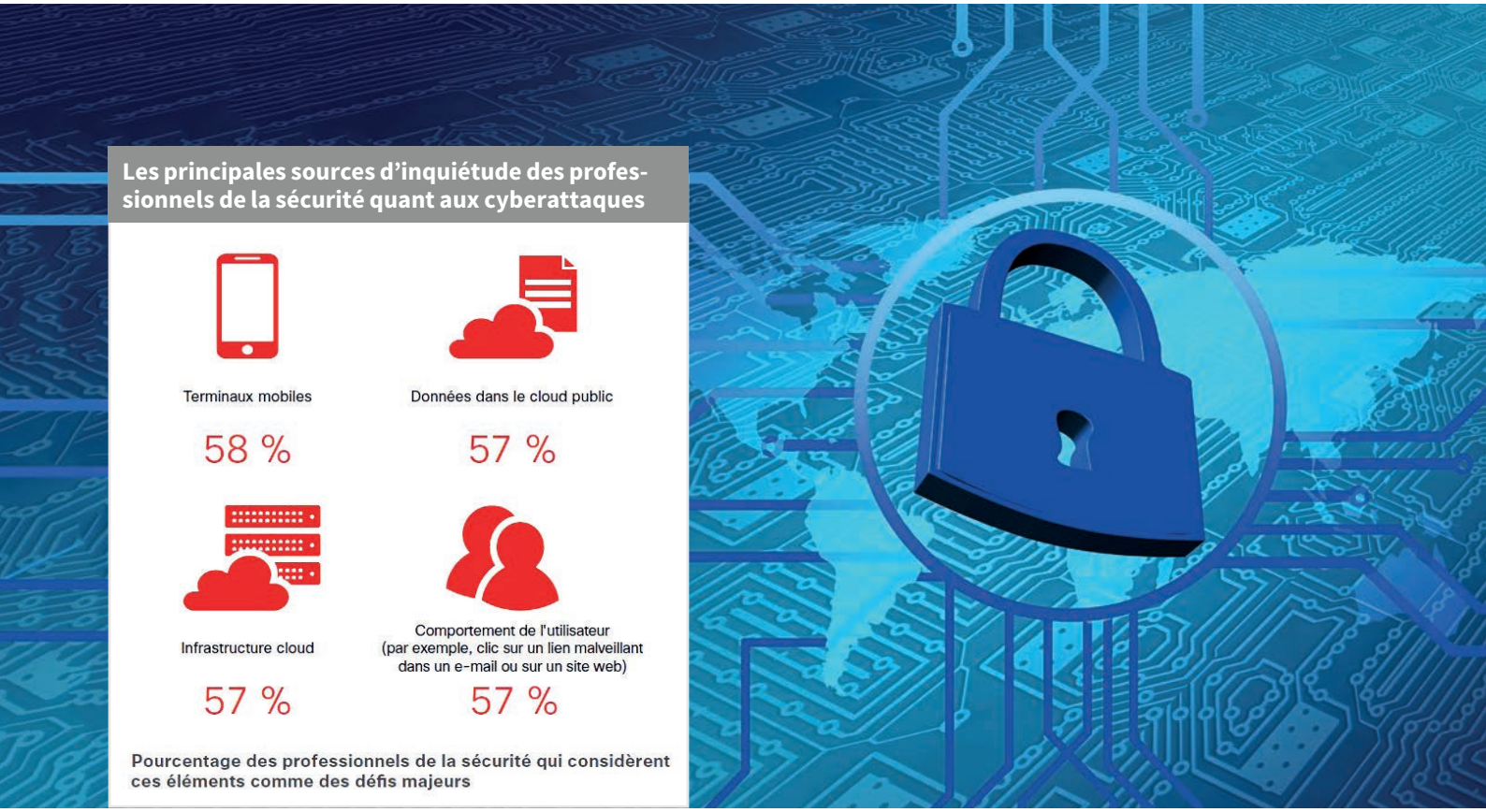
des applications Cloud tierces connectées au système d'information en 2016 ont présenté un risque de sécurité élevé.

Source : Cisco

Ce type d'attaque ne doit pas non plus nous faire oublier des attaques moins spectaculaires mais toutes aussi dévastatrices comme le ransomware WannaCry ou le malware Locky et ses multiples variantes qui se sont propagées, depuis un an, dans les entreprises de toutes tailles avec à la clé des pertes de données massives faute de mises à jour, de moyens de protection efficaces et l'absence de dispositifs de sauvegarde de données. Face à ces constats, la priorité des DSI semble désormais s'orienter vers la sécurité de leur système d'information. A ce titre, l'étude Carrières et Défis DSI en 2016, réalisée par le site lemondeinformatique.fr, place la sécurité en tête des priorités des directeurs IT. De même, IDC indique que les plus fortes progressions sur les dépenses en logiciels se feront sur la sécurité en 2017 (+8,6 %). Il faut dire que la sécurité fait face à un double défi : l'adoption d'un modèle plus efficace qui va au-delà de la simple sécurité périmétrique et des réglementations de plus en plus strictes et contraignantes des pouvoirs publics et européens.

a- Vers des outils de sécurité de nouvelle génération

Nous le savons, une sécurité efficace à 100 % n'existe pas. De ce fait, l'une des premières réponses des décideurs IT (RSSI et DSI) reste la sensibilisation auprès des utilisateurs. Des emailings, des réunions de tous les collaborateurs, des jeux de rôles, des simulations d'attaques, tout y passe pour sensibiliser les utilisateurs aux enjeux de la cybersécurité. En complément à cette sensibilisation auprès des utilisateurs, l'outillage reste bien sûr indispensable. Les solutions traditionnelles (antivirus, firewalls, UTM, etc.) garantissent aussi la sécurité périmétrique du SI. Mais là non plus, elles ne suffisent plus étant donné que le système d'information est de plus en plus ouvert et les données sont partout ; les responsables informatiques éprouvent de plus en plus de difficultés à garantir la sécurité de leur SI. Il est donc indispensable de compléter cet outillage par une sécurité centrée sur l'utilisateur, c'est clairement la tendance dans les entreprises face aux nouveaux usages. De plus en plus d'entreprises s'essayent d'ail-



Source : Enquête Cisco 2017 sur l'efficacité des mesures de sécurité

leurs à tester des nouveaux outils d'analyses comportementales des utilisateurs (UBA). En aucun cas, ces outils remplaceront les méthodes de sensibilisation des utilisateurs mais ils permettent, en s'aidant du machine learning et du big data, de détecter des signaux faibles, des anomalies au sein des systèmes d'information. Les éditeurs de ces solutions mettent souvent en avant la réduction des faux positifs, la diminution du temps de détection et, plus généralement, leur efficacité contrairement aux offres actuelles dont le fonctionnement repose sur un modèle vieillissant de signature. L'objectif de ces outils est aussi d'aider les entreprises à mieux appréhender les attaques et donner une réponse plus appropriée à cette cybercriminalité.

Logiciels malveillants les plus couramment observés

Décompte	
87 329	Applications potentiellement indésirables et fichiers binaires suspects
50 081	Injecteurs de chevaux de Troie (VBS)
35 887	Liens Facebook frauduleux
27 627	Téléchargeurs de chevaux de Troie (Scripts)
24 737	Redirection du navigateur (JS)
18 505	Redirection du navigateur - Téléchargements
15 933	Phishing (Liens)
14 020	Chevaux de Troie Android (Iop)
12 848	Redirection du navigateur
11 600	Piratages de profils Facebook
11 506	Blocages heuristiques (Scripts)
7712	Binaires compressés
5995	Téléchargeurs de chevaux de Troie (JS)
5510	Chevaux de Troie, méthodes heuristiques (Win32)
5467	Attaques iFrame du navigateur
4970	Android (Axent)
4584	Chevaux de Troie Android (Loki)
4398	Malwares (FakeAvCn)
3646	Chevaux de Troie (HideLink)
3006	Malwares (HappJS)

Source : Cisco Security Research

b- Des réglementations contraignantes mais nécessaires pour lutter contre la cybercriminalité

Entre protection des données personnelles et sécurisation drastique des équipements industriels, l'administration, qu'elle soit européenne ou nationale, fait désormais la loi. Déjà le Privacy Shield, validé le 12 juillet dernier par la commission européenne et qui remplace le Safe Harbor, est destiné à sécuriser le transfert de données personnelles des citoyens européens vers les Etats-Unis. Ensuite, beaucoup plus contraignant, le GDPR ou RGPD en français (Règlement général sur la protection des données), ce nouveau texte juridique européen, adopté en avril dernier par le parlement européen, fait office de référence en matière de protection des données à caractère personnel. Ce texte comprend des dizaines d'articles entrainant plus d'obligations juridiques que techniques à suivre pour les entreprises comme la protection des données personnelles collectées, l'analyse d'impact pour identifier les traitements susceptibles de présenter des risques particuliers pour les droits et libertés des personnes concernées, sans oublier la tenue du registre des traitements ou encore la preuve du respect des exigences personnelles. Il faut savoir qu'en cas de non-respect des règles du GDPR, des sanctions peuvent être infligées aux entreprises, à savoir des amendes pouvant atteindre 4 % du chiffre d'affaires de l'entreprise, jusqu'à un montant maximal de 20 millions d'euros. Il est donc vital pour les entreprises de commencer à se mettre en conformité dès à présent d'autant que ce texte doit entrer en vigueur dès 2018. Enfin, n'oublions pas les critères d'exécution des mesures de cybersécurité proposés par l'ANSSI et signés par le premier ministre pour les OIV (Opérateur d'importance vitale). La mission de l'ANSSI est donc d'accompagner ces opérateurs d'importance vitale dans la sécurisation de leurs systèmes d'information sensibles et d'éviter qu'une cyberattaque de grande ampleur, telle que l'a connu TV5 Monde en 2015, ne se reproduise. En France, plus de 200 opérateurs publics ou privés, dont les activités sont indispensables au bon fonctionnement du pays, sont classés OIV comme les entreprises liées au secteur de l'énergie (eau, nucléaire, etc.), à certaines industries, à l'armée en passant par la santé et la finance. ■

55 %

des responsables européens de la sécurité indiquent que le RGPD n'est pas une priorité majeure .

Source : Pierre Audoin Consultants (PAC)

General Data Protection Regulation

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

2. Les solutions Cisco : des nouveaux remparts pour lutter efficacement contre la cybercriminalité

« Chez Cisco, la cybersécurité est un axe de développement prioritaire pour protéger la transformation digitale actuellement opérée par les entreprises. *De par notre large couverture fonctionnelle en matière de cybersécurité, Cisco possède une vision globale et architecturale pour prévenir les entreprises des menaces de plus en plus sophistiquées* », souligne Alain Dubas, directeur des opérations commerciales Cybersécurité pour la France et l'Europe du Sud. En effet, la transformation numérique et la nouvelle manière de consommer les services (Cloud, mobilité, web, etc.) ont ouvert de nouvelles opportunités d'attaques pour les cybercriminels lesquels sont toujours mieux organisés pour nuire aux entreprises. De leur côté, les entreprises peuvent toujours compter sur leurs firewalls qui constituent toujours la première ligne de défense pour les accès entrants, mais face aux menaces qui vont bien au-delà du périmètre de sécurité du système d'information, les entreprises ont besoin aujourd'hui de comprendre ces menaces. Elles ont aussi besoin d'efficacité, d'intégration, d'anticipation et de réactivité. « *Il y a trois mois, j'ai rencontré une banque qui disposait de 50 solutions de sécurité différentes, cette hyper-fragmentation engendre une grande complexité (multiplicité des contrats de maintenance) et un manque de réactivité face aux menaces. Pour leur apporter une réponse adéquate, Cisco attache donc une grande importance à positionner l'architecture de ses solutions afin qu'elles soient intégrées, automatisées et qu'elles discutent les unes avec les autres même avec des applications tierces. Cela dit, aucune solution de sécurité du marché ne peut stopper l'ensemble des attaques mais notre objectif, grâce à notre portfolio, est d'améliorer le temps de détection d'une attaque pour apporter la réponse appropriée et le rôle d'un partenaire intégrateur comme DCI est important pour comprendre les enjeux et l'écosystème de sécurité des entreprises* », résume Alain Dubas. Et de conclure : « *Pour lutter contre la cybercriminalité, notre stratégie s'oriente vers des solutions dans le Cloud. Et ces applications sont héritées de rachats successifs menés par Cisco depuis plusieurs années. D'ici la fin de l'année 2017, une refonte majeure de nos offres Cloud sera portée sous une marque unique Umbrella et via une seule console de management Cisco Defense Orchestrator.* » ■

© J. David

> **Cisco possède une vision globale et architecturale pour prévenir les entreprises des menaces de plus en plus sophistiquées.**
>
> **Alain Dubas,** directeur des opérations commerciales Cybersécurité pour la France et l'Europe du Sud

Quatre solutions de la gamme de produits Cisco pour lutter efficacement et de bout en bout contre la cybercriminalité :

1- AMP (Advanced Malware Protection) : pour contrer les attaques avancées

AMP est une technologie de détection sans moteur qui agit sur les endpoints, les solutions réseaux (Firewall, IPS, routeur) et les passerelles (web et emails). AMP détecte et bloque les programmes malveillants, analyse le réseau en continu et crée des alertes rétrospectives. Ces dernières, qui indiquent la nature et la compréhension de circulation d'un fichier infecté, sont rendues possibles par trois fonctionnalités :

- **L'évaluation de la réputation des fichiers (analyse des fichiers en ligne pour les bloquer ou appliquer des politiques)**
- **Le sandboxing des fichiers (analyse des fichiers inconnus pour en comprendre le véritable comportement)**
- **L'analyse rétrospective des fichiers (suivi des fichiers en cas de modification de la réputation d'un fichier)**

Pour assurer son efficacité, AMP tire parti du centre de recherche Cisco Talos qui regroupe plus de 250 chercheurs et d'experts et qui bloque plus de 20 milliards de menaces par jour. Ce groupe a donc pour objectif de combattre le monde de la cybercriminalité. Les missions de cette unité de recherche sont d'analyser et d'identifier tous les types de menaces et les vulnérabilités, mais aussi de s'engager dans des actions spécifiques visant à détruire les sources de ces menaces. Par exemple, Talos a montré son efficacité en travaillant en partenariat avec un hébergeur pour stopper le trafic de l'Exploit Kit Angler qui délivrait des ransomwares et rapportait 30 millions de dollars par an à ses auteurs. « *Surtout avec Talos, nous avons diminué le temps de détection de plusieurs dizaines de jours à quelques heures, de l'ordre de 13 heures à la fin de l'année 2016* », précise Jean-Baptiste Guglielmine, consultant sécurité Cisco.

Avec Talos, nous avons diminué le temps de détection de plusieurs dizaines de jours à quelques heures, de l'ordre de 13 heures à la fin de l'année 2016.

Jean-Baptiste Guglielmine,
consultant sécurité Cisco

Pour les entreprises qui ont choisi AMP, les bénéfices sont multiples :

- **Une protection efficace avant, pendant et après l'attaque**
- **Un accès aux informations détaillées**
- **Un contrôle précis des politiques**
- **Une vision globale pour les utilisateurs grâce des fonctions d'analytique prédictive**
- **Un accompagnement de l'expertise Cisco dans la cybersécurité**

Pour plus d'informations : http://www.cisco.com/c/fr_fr/solutions/enterprise-networks/advanced-malware-protection/index.html

2- Umbrella : pour superviser et protéger partout

Hérité du rachat d'OpenDNS par Cisco, Umbrella est un service de sécurité qui opère en amont sur la couche DNS pour stopper les requêtes issues d'adresses IP ou de domaines malveillants avant l'établissement d'une connexion. Ainsi, les nombreux terminaux qui n'utilisent pas de proxy, notamment les objets connectés, peuvent être bloqués et protégés. Le fonctionnement d'Umbrella se fait en trois temps :

- **Il identifie les infrastructures d'attaques avant leur utilisation**
- **Il donne une visibilité unique pour tous les accès**
- **Il bloque les menaces avec l'établissement de la connexion**

Techniquement, Umbrella autorise la connexion pour les requêtes autorisées et non dangereuses. Il permet aussi le blocage des connexions non désirées ou dangereuses faites par le client ou un malware et il peut effectuer un contrôle de contenu via proxy Cloud pour les cas où une investigation plus poussée est nécessaire. « *Par exemple, avec Umbrella, il est même possible de reconnaître, voir de prédire, des domaines malicieux grâce aux patterns de trafic constatés ou grâce aux analyses des algorithmes de génération de domaine. L'outil Investigate quant à lui permet de consulter cette base* », indique Jean-Baptiste Guglielmine, consultant sécurité Cisco. En effet, Investigate fournit des informations sur les domaines, les IP et les malwares visibles sur Internet, produit un graphe en temps réel des requêtes DNS et d'autres données contextuelles et enrichit les données de sécurité avec une intelligence globale.

Pour plus d'informations :
https://umbrella.cisco.com/products/features

3- CloudLock : pour sécuriser les environnements Cloud

CloudLock répond parfaitement aux usages actuels en matière de sécurité Cloud, à savoir l'implémentation de solutions CASB (Cloud access security brokers) pour répondre à la sécurisation des services Cloud de type SaaS, IaaS et PaaS. Hérité d'un rachat en 2016 par Cisco, CloudLock suit et gère les comportements des utilisateurs et des données sensibles dans les applications Cloud, et pour ce faire, il exploite les API des différentes applications.

CloudLock agit donc sur trois cibles :

- **La sécurité des utilisateurs**

Pour protéger les utilisateurs, CloudLock exploite des techniques de machine learning qui détectent les anomalies suivant plusieurs facteurs. L'outil analyse et repère aussi les activités en dehors des pays cités sur la liste blanche.

- **La sécurité des données**

CloudLock renferme un module de prévention des pertes de données (DLP) qui supervise en permanence les environnements Cloud et détecte les informations sensibles. Précisons que ce module propose des politiques clés en main, paramétrables et personnalisables.

- **La sécurité des applications**

CloudLock agit comme un pare-feu pour contrôler les applications Cloud malveillantes connectées au système d'information de l'entreprise. De plus, CloudLock fournit un indice de confiance (basé sur les informations provenant de la communauté) qui autorise ou bloque les applications Cloud en fonction des risques identifiés.

Pour plus d'informations :
http://www.cisco.com/c/fr_fr/products/security/cloudlock/index.html

4- Stealthwatch : pour disposer d'une plus grande visibilité du réseau

Suite au rachat de Lancope en 2015, éditeur de l'application Stealthwatch, Cisco ajoute à son catalogue une solution de sécurité adaptative qui offre une visibilité complète avant, pendant et après les attaques (malwares, DDoS, menaces persistantes avancées et menaces internes). Stealthwatch surveille également en permanence le réseau interne pour détecter les activités des cybercriminels, pour cela, l'outil s'appuie sur le protocole Netflow. A ce titre, en associant les analyses détaillées des flux fournies par IOS Flexible NetFlow aux données contextuelles issues du moteur de services Identity Cisco et à Stealthwatch, les entreprises peuvent détecter en temps réel dans toute l'infrastructure les activités malveillantes, les mouvements de données anormaux, les trafics suspects et les menaces avancées. D'un point de vue fonctionnel, Stealthwatch génère des indicateurs et suivant leur importance, prend des décisions comme une mise en quarantaine par exemple.

Parmi les bénéfices de Stealthwatch, citons :

- **Une visibilité étendue sur le réseau**

En collectant des données sur l'infrastructure de réseau, Stealthwatch fournit des informations essentielles sur le trafic du réseau, notamment les adresses IP d'origine et de destination, les volumes de trafic transmis et des données sur les utilisateurs, les terminaux et les applications. Résultat : toutes ces informations procurent une vision assez précise des comportements normaux et anormaux dans l'entreprise.

- **Un traitement accéléré des incidents**

Stealthwatch transforme les données issues de NetFlow et d'autres sources en informations exploitables afin d'accélérer le traitement des incidents. L'application réduit les délais de réponse, limitant le dépannage à quelques minutes, contre plusieurs jours, voire plusieurs mois avec d'autres solutions de sécurité.

- **Des enquêtes plus rapides et plus précises**

Stealthwatch peut stocker des données relatives au réseau pendant des mois, voire des années, ce qui représente une piste d'audit inestimable. Stealthwatch se révèle donc indispensable pour réaliser des enquêtes techniques plus rapides et plus précises après l'incident.

- **Une amélioration de la segmentation et un respect de la conformité**

En travaillant avec Cisco ISE (Identity Services Engine) et Cisco TrustSec, la solution Stealthwatch segmente au mieux les ressources réseau essentielles et surveille les politiques d'utilisation afin de renforcer le contrôle des accès et des systèmes de protection.

Pour plus d'informations :
http://www.cisco.com/c/fr_fr/products/security/stealthwatch/index.html

3. DCI, votre partenaire à valeur ajoutée sur la cybersécurité

La majorité des entreprises ont fait de la lutte contre la cybersécurité un enjeu prioritaire. Et pourtant, en interne, pendant très longtemps ces questions de sécurité ont été et sont toujours, dans la majorité des cas, gérées par la DSI sur des problématiques liées uniquement à l'IT. Toutefois, les attaques de ces dernières années ont prouvé que cette problématique concerne tous les collaborateurs dans l'entreprise, une vraie prise de conscience sur ce sujet est d'ailleurs en train d'émerger. Mais cette lutte coûte chère, elle nécessite pour les entreprises de disposer de ressources financières, techniques, juridiques et humaines de plus en plus importantes. Et aujourd'hui, en ont-elles vraiment les moyens ? Pas si sûr, du moins pas toutes seules... Les entreprises doivent donc se faire accompagner par de vrais professionnels de la cybersécurité comme DCI, l'un des spécialistes du secteur. Avec ses 25 années d'expériences, DCI a su se positionner sur les services numériques avec un axe fort d'engagement sur la sécurité et la cybersécurité. Acteur reconnu auprès de ses clients et de ses partenaires fournisseurs comme Cisco, DCI réalise d'ailleurs 40% de son chiffre d'affaires (57 M€) dans ce secteur. ■

DCI réalise 40 % de son chiffre d'affaires dans la cybersécurité.

Nicolas Berchoux, directeur du développement business chez DCI et **Jean Nemeth,** expert cybersécurité chez DCI

Sur le terrain, comment réagissent les entreprises face aux nouvelles lois réglementaires (RGPD, loi de programmation militaire, etc.) ?

Nous constatons que les entreprises ne sont pas forcément prêtes sur toutes ces nouvelles réglementations, notamment le RGPD qui sera opérationnel en mai 2018. Le RGPD, un nouveau règlement européen autour de la protection des données personnelles, renferme à la fois des processus juridiques et des critères techniques (ndlr : essentiellement l'article 32). Notre rôle est d'accompagner les entreprises avec des vrais spécialistes dans leur démarche globale du respect de la RGPD à la fois sur ces questions techniques mais aussi sur les aspects juridiques en les orientant vers les bons interlocuteurs. De même, concernant la protection des opérateurs d'importances vitales - OIV (loi de programmation militaire), nous mettons déjà en avant les exigeances formalisées par l'ANSSI (Agence nationale de la sécurité des systèmes d'information). De plus, nous avons entrepris les démarches nécessaires à la certification ISO 27001 de notre N-SOC.

> **DCI est certifié sur l'ensemble des solutions technologiques citées dans ce livre blanc.**
>
> **Nicolas Berchoux,** directeur du développement business chez DCI

Les entreprises sont-elles suffisamment armées aujourd'hui pour lutter efficacement contre la cybercriminalité ? Et disposent-elles de moyens financiers ?

Les entreprises sont davantage sensibilisées au vu des incidents majeurs rapportés par la presse. Résultat : nos clients sont toujours plus nombreux à souhaiter réaliser des audits sur la sécurité de leur infrastructure. Mais les audits que nous avons mené sur le terrain nous permettent de constater que les entreprises ne sont pas suffisamment outillées. Bien sûr, elles le sont pour la protection de leur périmètre mais pour tout ce qui se trouve en dehors de leur périmètre, elles sont souvent démunies. En effet, à l'heure où les solutions Cloud et la mobilité se démocratisent, il est essentiel d'aller vers l'implémentation de solutions telles que les technologies CASB (Cloud access security brokers) pour répondre à la sécurisation de ces nouveaux usages. Pour le budget sécurité, les entreprises françaises mettent souvent les moyens lorsque l'attaque est déjà en place. On est donc souvent dans la réaction à une attaque plus que dans l'anticipation de la menace. Là aussi, notre rôle est de les aider à adopter une démarche proactive dans leur sécurité.

Concrètement, par quels types d'outils passe la sécurisation de ces nouveaux usages ?

Comme je vous le citais précédemment, une sécurité accrue des nouveaux usages se justifie par l'intégration d'un écosystème de sécurité global. Ce dernier doit s'appuyer sur différents outils communiquants entre eux, tels que le CASB, le User Behaviour Analytics, l'authentification des accès, des outils de chiffrement et des applications d'analyses comportementales. A ce titre, le SIEM (Security information and event management) est également amené à prendre un essor plus important.

Au-delà des aspects purement produit, il est important de pouvoir compter sur un prestataire de services disposant d'un retour d'expérience significatif. Cela permet d'assurer un maintien en condition de sécurité optimal et de façon durable. Cela passe par la réalisation d'audits réguliers, d'un suivi d'exploitation permettant de s'assurer de la tenue à jour des équipements mais aussi des règles de sécurités mises en œuvre, tout autant que des capacités à proposer des services managés permettant de disposer du meilleur des compétences à tout moment. En effet, il est de plus en plus difficile pour un client de disposer des compétences et de ressources nécessaires à la détection et à la remédiation des attaques. L'expertise d'un spécialiste de ce genre de missions prend alors tout son sens.

Au-delà de l'aspect produit, il est important de pouvoir compter sur le suivi et les services apportés par DCI.

Jean Nemeth,
expert cybersécurité chez DCI

En tant que partenaire Cisco, comment définiriez-vous votre rôle ?

DCI est un acteur reconnu depuis de nombreuses années sur le marché de la sécurité. Notre partenariat avec Cisco (Partenaire Premier), établi depuis plus de 5 ans et axé autour de domaines de compétences spécifiques fortes sur les solutions de la marque nous amène légitimement à mettre en œuvre les solutions de sécurité du constructeur. DCI est d'ailleurs déjà certifié sur l'ensemble des briques technologiques mentionnées précédemment par Alain Dubas et Jean Baptiste Guglielmine.

Comment assurez-vous le suivi et le cycle de vie de l'écosystème de sécurité ?

DCI s'est équipé d'un centre de support opéré par nos soins depuis notre siège situé en France, aux Ulis et composé de 30 personnes sans compter les équipes d'ingénieurs et d'intégration qui peuvent intervenir en appui. Ce centre de support nous permet de superviser et administrer la sécurité de nos clients. Aujourd'hui, nous sommes déjà capables d'assurer la continuité de service de nos clients 24h/7j sur site et à distance. A terme, nous souhaitons structurer notre plateforme afin d'y adjoindre de nouveaux services et outils de sécurité nécessaires pour faire face aux nouvelles menaces qui ne cessent de se développer.

Pour plus d'informations : http://www.dci.fr/